



MATTHEW D. SKIPPER

[WWW.SKIPPERLAWLLC.COM](http://WWW.SKIPPERLAWLLC.COM)

443-274-6106  
fax 443-292-4735  
[matt@skipperlawllc.com](mailto:matt@skipperlawllc.com)

2110 Priest Bridge Drive, Suite 2  
Crofton, MD 21114

JEFFREY A. KAHNTROFF, ASSOCIATE  
RICHARD R. TRUNNELL, Of Counsel  
Wes P. HENDERSON, Of Counsel

August 15, 2017

**VIA EMAIL and FIRST CLASS MAIL**

Jeff Karberg  
Administrator of the Identity Theft Program  
Office of the Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
[Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us)

RE: Ransomware attack on Skipper Law, LLC  
Date: 11 August 2017

Dear Mr. Karberg:

We are contacting you to inform you of Ransomware that reached our system on August 11, 2017 at 7:43a.m.. Our informational security technician has reviewed the system and is fairly certain that no files or personal information were or will be opened or copied. Nonetheless, we wanted to email you out of an abundance of caution to let you know of the incident.

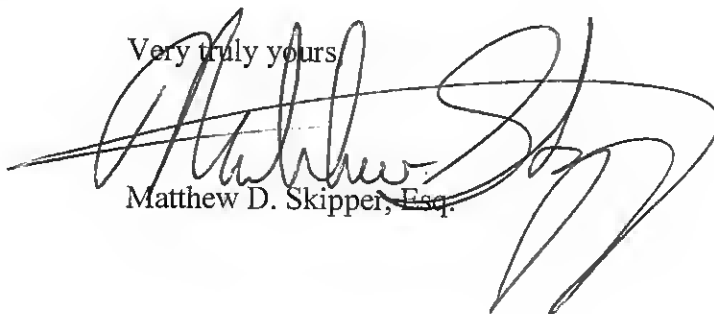
Specifically, on the morning August 11, 2017, a bot which had been continuously attempting to access our system got access to our Intern login through our remote connection. Our investigation revealed that once the Ransomware entered our system, it placed an encryption lock on client files. The attacker then requested a ransom to unlock the files. However, the attacker either never opened the files, or if it did, it afterwards deleted the cache to erase any trace of accessing the files. Based on research of Ransomware attacks to other firms and the investigation of our system and files, we conclude it is unlikely that any personal information was accessed, copied, or opened. We did not pay or contact the attacker.

The Intern profile only had access to our case files; it did not have access to our administrative files. Further, we maintain our clients' personal information on Clio, a web-based client, not on our server. The attack did not provide access to Clio. What the client files contain varies depending on case type. Most did not contain any personal information other than the client names. In a few cases, medical records, social security numbers,

and date of birth were in the client files. Specifically, a large portion of our practice is consumer protection, and those files usually just contain name and address, and occasionally date of birth. For our personal injury clients, the files often contain medical records. For our business clients, matters in discovery often include corporate documents and occasionally company tax returns. We believe that the accessible files consisted of 199 Maryland residents.

In response to the attack, we quarantined all infected files and ran a data restore mechanism as well as accessing our data back-up. After the incident, we also contacted a specialist to discuss strengthening our security, and have made sure everyone's password is reasonably difficult for a bot to access, as this was the source of the attack. Attached is a sample of the letter that we are sending to all clients.

If you have any questions, please do not hesitate to contact me directly by phone or email.

Very truly yours,  
  
Matthew D. Skipper, Esq.